REMARKS

The Applicants and the undersigned thank Examiner Norris for his careful review of this application. Consideration of the present application is respectfully requested in light of the above amendments to the claims and in view of the following remarks. Claims 1-5, 9, 10, and 12-16 have been rejected and Claims 6-8 and 11 have been objected to. Applicants have amended Claims 2-12 and 15. Applicants have canceled Claims 1, 13-14, and 16. Applicants have added Claims 17-52. Upon entry of the amendments, Claims 2-12, 15, and 17-52 are pending in the subject application with none having been allowed. The independent claims for this application are Claims 2, 17, 24, 32, 39, and 46.

I. Claim Rejections Under 35 U.S.C. § 103(a)

The Examiner rejected Claims 2, 4, 5, 9, 10, 15, and 16 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 6,301,668 to Gleichauf, et al. ("*Gleichauf*") in view of U.S. Patent No. 6,324,647 to Bowman-Amuah. ("*Bowman*"). The Examiner rejected Claim 3 under 35 U.S.C. § 103(a) as being unpatentable over the *Gleichauf/Bowman* combination in view of U.S. Patent No. 6,519,647 to Howard, et al. ("*Howard*"). The Examiner rejected Claims 13 and 14 under 35 U.S.C. § 103(a) as being unpatentable over the *Gleichauf/Bowman* combination in view of U.S. Patent No. 6,415,321 to Gleichauf, et al. ("*Gleichauf 321*"). The Applicants respectfully offer the following remarks to traverse these pending rejections.

A. Independent Claim 2, as Amended, is Distinguishable from *Gleichauf* in View of *Bowman*

The rejection of independent Claim 2 is respectfully traversed in view of the submitted amendments. It is respectfully submitted that *Gleichauf* in view of *Bowman* fails to teach or suggest all of the recitations enumerated in Claim 2, as amended. The Examiner alleges that *Gleichauf* discloses all of the limitations of Claim 2 except for a help file, which contains on-line help information on a computer. *Office Action*, at p. 4. The Examiner further alleges that *Bowman* discloses the limitation of a help file that contains on-line help information on a computer. *Id.* Applicants respectfully assert that the *Gleichauf/Bowman* combination fails to teach or suggest each and every element of amended Claim 2.

1. *Gleichauf* Fails to Teach or Suggest a Pluggable Express Update Package Comprising Exploits.

Gleichauf fails to teach or suggest a scanner receiving a pluggable express update package comprising exploits recited by amended Claim 2. *Gleichauf* teaches a scan engine capable of receiving **network information** that is retrieved from a network map by a domain mapping service. *Gleichauf*, col. 6:15-20. Alternatively, *Gleichauf* teaches a scan engine capable of receiving network information directly from the network. *Gleichauf*, col. 5:52-54. The network information is retrieved by the scan engine by scanning devices on an internal network, collecting banners from port scans, and analyzing the banners to discover the network information. *Gleichauf*, col. 5:54-59. The network information received by the scan engine includes the devices coupled to the network, the operating systems on those devices and the services available on each device. *Gleichauf*, col. 5:59-62. The scan engine then compares the network information with a rules set to determine potential vulnerabilities. *Gleichauf*, col. 5:62-6:4; *see also* U.S. Patent No. 6,324,656 to Gleichauf, et al. (formerly U.S. Patent Application No. 09/107,964).

In contrast to *Gleichauf* amended Claim 2 requires a pluggable express update package that is configured as an independent plug-in module that is separate from the scanner. The update package of amended Claim 2 comprises exploits that check a host computer system for security vulnerabilities. An exploit can be an individual security check for a computer system. *Application* at 2:24-25. Further, the plug-in module comprising the update package communicates with the scanner to support vulnerability assessments conducted by the scanner.

The network information of *Gleichauf* is not the same or equivalent to the pluggable express update package comprising exploits of amended Claim 2. The exploits of amended claim 2 check a host computer system for security vulnerabilities. On the other hand, the network information of *Gleichauf* comprises an inventory of devices and systems on a computer network. The network information of *Gleichauf* does not check the host computer system for security vulnerabilities. Instead, *Gleichauf* teaches that the network information is analyzed by the scan engine to determine potential vulnerabilities. While the rules set used by the scan engine to analyze the network information of *Gleichauf* may be characterized as an exploit, *Gleichauf* fails to teach or suggest obtaining and running these exploits from the update recited by Claim 2. Instead, *Gleichauf* teaches receiving the network information, and not the code used

by the scan engine to analyze it.

2. *Gleichauf* Fails to Teach or Suggest a Pluggable Scanner Separate From and Capable of Receiving Updated Exploits for Vulnerability Assessment

Gleichauf fails to teach or suggest receiving an update package configured as an independent plug-in module that is separate from the scanner and communicates with the scanner to support the vulnerability assessments conducted by the scanner, as set out in the recitation of amended Claim 2. *Gleichauf* teaches a scan engine comprising software code executing remotely from the network security system. *Gleichauf*, col. 5:27-30. The network security system is a typical intrusion detection system. *Gleichauf*, col. 5:1-4. Conversely, the scan engine conducts a vulnerability assessment of the network. *Gleichauf*, col. 5:62-6:4. An intrusion detection system attempts to identify data that may be attacking the system now, while a vulnerability assessment analyzes the network to determine what type of data may harm the system in the future. Thus, while the software code of the scan engine in *Gleichauf* is separate from the intrusion detection system it is not separate from the scanner.

On the other hand, amended Claim 2 teaches a method whereby exploits used to conduct vulnerability assessment are received in an express update package that is configured as an independent plug-in module separate from the scanner. Prior to the invention of amended Claim 2, exploits were hard-coded on the scanner. Hard-coding prevented a user from modifying or adding exploits to be used by that scanner for vulnerability assessment. Maintaining a separation between the scanner and the exploits in the express update package of amended Claim 2 allows exploits to be added or updated and used by the scanner without need for replacing the scanner itself. *See Application* at 2:33-34. Unlike Gleichauf, the invention of independent Claim 2 comprises a process whereby a capability of the scanner to conduct vulnerability assessments is updated by obtaining a pluggable express update package. The express update package is a plug-in module that communicates with the scanner to support the vulnerability assessments. The plug-in module is separate from the scanner and comprises exploit objects for exploits that check for security vulnerabilities.

Thus, *Gleichauf* fails to teach or suggest receiving an update package, comprising exploits, configured as an independent plug-in module that is separate from the scanner and communicates with the scanner to support the vulnerability assessments conducted by the scanner. While *Gleichauf* does teach that the software code for the scan engine can be separate

from the intrusion detection system, it is not separate from the scanner, which conducts vulnerability assessment. Furthermore, as has been shown in section 1 above, while *Gleichauf* teaches network information that is separate from the scan engine, the network information is not the same or equivalent to an express update package comprising exploits.

3. *Gleichauf* Does Not Teach or Suggest Resources, Help Information, or Exploit Attribute Information Maintained Separate from the Exploits to Support Independent Updating

Gleichauf fails to teach or suggest resources maintained as resource objects separate from the exploits of the exploit objects to support an independent updating of the resource objects and the exploit objects, as set out in the recitation of amended Claim 2. *Gleichauf* also fails to teach or suggest a dat file comprising exploit attribute information that is stored in a file separate from the exploit objects to support an independent updating of the dat file and the exploit objects, as recited in amended Claim 2. Further, *Gleichauf* fails to teach or suggest a help file comprising on-line help information stored in a file separate from the exploit objects to support an independent updating of the help file and exploit objects, as set out in amended Claim 2. The exploits of amended Claim 2 check the host computer system for security vulnerabilities, while the resources are used by the scanner. The exploit attribute information defines attribute information for the exploits of the exploit plug-in module. The help file comprises on-line help information about the exploits of the exploit plug in module.

Gleichauf teaches a scan engine sending a request to a domain mapping service. *Gleichauf*, col. 6:14-15. The domain mapping service maintains a network map, which comprises a compilation of network information. *Gleichauf*, col. 6:15-17. In response to the request from the scan engine, the domain mapping service sends the compilation of network information from the network map to the scan engine. *Gleichauf*, col. 6:17-19. In the alternative, the scan engine of *Gleichauf* can retrieve the information from a network map comprising a multi-dimensional database. *Gleichauf*, col. 6:5-14. While *Gleichauf* does teach that the network information used by the scan engine is maintained together in the compilation, and the network map is maintained in a database, it does not teach or suggest that the resources exploit attribute information, or the help file are maintained separate from the exploits. Maintaining the resources, exploit attribute information, and help file separate from the exploits allows for the updating of those files independent of an update to the exploits.

In *Gleichauf*, the information retrieved from the network map or the domain mapping

service comprises the information that is analyzed by the scan engine to determine potential vulnerabilities. *See Gleichauf*, col. 5:62-65 On the other hand, the exploits of amended Claim 2 check the host computer system for security vulnerabilities, the resources are used by the scanner, and exploit attribute information defines attribute information for the exploits of the exploit plug-in module, and the help file comprises on-line help information about the exploits. Thus, the exploits, resources, exploit attribute information, and help file are used by the scanner to assist the scanner in analyzing a host computer system, while the network information of Gleichauf is that which is analyzed by the scanner. Therefore, *Gleichauf* fails to teach or suggest resources maintained as resource objects separate from the exploits of the exploit objects to support an independent updating of the resource objects and the exploit objects. Further, *Gleichauf* fails to teach or suggest exploit attribute information or a help file comprising on-line help information that are stored in a file separate from the exploit objects to support an independent updating of the dat file or the help file and the exploit objects, as recited in amended Claim 2.

4. *Bowman* Does Not Teach or Suggest a Pluggable Express Update Package Comprising a Help File

The Examiner asserts that *Bowman* teaches or suggests the limitation of claim 2, wherein the pluggable express update package comprises a help file comprising on-line help information, about the exploits of the exploit plug-in module. *Office Action* at p. 4. However, neither the section that the Examiner directs Applicants' attention to, nor any other portion of *Bowman*, teaches a help file containing on-line help information about the exploits, as required by amended Claim 2. The help file of amended Claim 2 comprises on-line help information about the exploits in the exploit plug-in module of the express update package. The help file of amended Claim 2 is stored in a file separate from the exploit objects, thereby supporting the ability to independently update the help file and the exploit objects.

In support of his assertion, the Examiner directs Applicants' attention to a portion of *Bowman* that teaches the use of JAVA and ActiveX technologies to create server applications by embedding software in hypertext markup language ("HTML") pages. *Bowman*, col. 9:30-50. While the use of HTML pages may show that *Bowman* teaches the use of on-line technology, the server applications are not help files comprising on-line help information about the exploits.

Therefore, the Examiner has not shown that *Bowman* teaches or suggest a help file comprising on-line help information about the exploits of the exploit plug-in module.

Therefore, Applicants' have shown that *Gleichauf*, in combination with *Bowman*, fails to teach or suggest all of the recitations enumerated in amended Claim 2. Accordingly, reconsideration and withdrawal of the rejection of amended Claim 2 is respectfully requested.

The Inventions of Dependent Claims 3-12, and 15 are Distinguishable from the Cited Art

The Applicants respectfully submit that the above-identified dependent claims are allowable because the independent claim from which they depend, amended Claim 2 is patentable over the cited references. The Applicants also respectfully traverse the Examiner's assertions about these claims and submit that the recitations of these dependent claims are of patentable significance. The Applicants respectfully request that the Examiner reconsider and withdraw the pending rejection of Claims 3-5, 10, and 12-15.

II. Objections for Claims Depending From a Rejected Base Claim

The Examiner has objected to Claim 6-8 and 11 as being dependent upon rejected base claims. Claim 6-8 and 11 ultimately depend from independent Claim 2, as amended. Applicants, in the above paragraphs, have successfully traversed all rejections to amended Claim 2. In view of the foregoing, Applicants respectfully request that the Examiner withdraw the present objections to amended dependent Claims 6-8 and 11.

III. Addition of New Claims 17-54

The Applicants and the undersigned thank Examiner Norris for noting that claims 6-8 and 11 contain allowable subject matter. Applicants have added new independent Claims 17, 24, 32, 39, and 46, and dependent Claims 18-23, 25-31, 33-38, 40-45, and 47-52. Independent Claim 17 is equivalent to original Claim 6, rewritten in independent form to include limitations of original independent Claim 2 and the original intervening claims. Independent Claim 24 is equivalent to original dependent Claim 11, rewritten in independent form to include limitations of original independent Claim 2 and the original intervening claims.

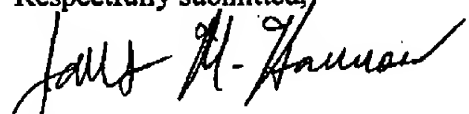
Independent Claim 32 comprises subject matter of independent Claim 2 and dependent Claims 4 and 6, including the allowable subject matter noted by the Examiner in Claim 6. Independent Claim 39 comprises subject matter of independent Claim 2 and dependent Claims 4 and 6, including the allowable subject matter noted by the Examiner in Claim 6. Independent Claim 46 comprises subject matter of independent Claim 2 and dependent Claims 9-11, including the allowable subject matter noted by the Examiner in Claim 11. Applicants and the undersigned respectfully request that independent Claims 17, 24, 32, 39, and 46 and the claims that depend from them be passed to allowance. The new claims find clear support in the specification and do not contain new matter.

CONCLUSION

The foregoing is submitted as a full and complete response to the Official Action mailed on January 30, 2004. The Applicants have amended the claims and have submitted remarks to traverse the objections and rejections of pending Claims 2-12, 15, and 17-52. The Applicants have shown above that Claims 2-12, 15, and 17-52 are allowable over the art cited by the Examiner and respectfully request that the Examiner withdraw all pending rejections and/or objections to Claims 2-12 and 15.

If the Examiner believes that there are any issues that can be resolved by a telephone conference, or that there are any informalities that can be corrected by an Examiner's amendment, a telephone call to the undersigned at (404) 572-4691 to discuss same is respectfully requested.

Respectfully submitted,



James M. Hannon
Reg. No. 48,565

KING & SPALDING LLP
45th Floor
191 Peachtree Street
Atlanta, Georgia 30303
404.572.4691
KS# 05456.105002